



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

09/608,123

06/30/2000

Martin J. Pagel

1817P

1033

7590

03/07/2006

Sawyer Law Group LLP  
PO Box 51418  
Palo Alto, CA 94303

EXAMINER

COLIN, CARL G

ART UNIT

PAPER NUMBER

2136

DATE MAILED: 03/07/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	Application No. 09/608,123	Applicant(s) PAGEL, MARTIN J.	
	Examiner Carl Colin	Art Unit 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 05 December 2005.
- 2a) ☒ This action is **FINAL**.                      2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 28-31 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 28-31 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 30 June 2000 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on \_\_\_\_\_ is: a) ☐ approved b) ☐ disapproved by the Examiner.  
If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

**Priority under 35 U.S.C. §§ 119 and 120**

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
a) ☐ All b) ☐ Some \* c) ☐ None of:  
1. ☐ Certified copies of the priority documents have been received.  
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).  
\* See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).  
a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)                  | 4) <input type="checkbox"/> Interview Summary (PTO-413) Paper No(s). _____  |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)         | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ | 6) <input type="checkbox"/> Other: _____                                    |

## **DETAILED ACTION**

### ***Response to Arguments***

1. In response to communications filed on 12/5/2005, applicant amends claim 28. The following claims 28-31 are presented for examination.

1.1 Applicant's remarks, pages 4-11, filed on 12/5/2005, with respect to the rejection of claims 28-31 have been fully considered but they are not persuasive. Applicant has amended independent claim 28 to expressly recite that the master and the secret keys are received "from a distribution center over a network after manufacture". This limitation constitutes new matter as discussed further below. Applicant states "since the PGD is coupled between a distribution center and a distribution center the distribution of the keys over the network clearly occurs after the PGDs have been manufactured. Examiner respectfully disagrees. A transmission over a telecommunication network to a postage device does not equate that the transmission is after the transmission of the manufacture of the device. In addition, the claimed limitation recites "receiving ...after manufacture". It is not definite what applicant means by after manufacture. The claim does not clearly state what is manufactured. Applicant states that Baker fails to teach that meters in each group destination also receive a secret corresponding to that group destination as required by step (a). In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., that meters in each group destination also receive a secret corresponding to that group destination as required by step (a)) are not recited in the rejected claim(s). Although the claims

are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). Applicant states that Baker's master key is not analogous to the claimed invention because key is not received after manufacturing. Examiner respectfully disagrees for at least the reasons mentioned above. Applicant has not overcome the rejection by amending the claims. Therefore, it remains the Examiner's position that claims 58-62 are still rejected in view of the same references.

***Claim Rejections - 35 USC § 112***

2. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

2.1 Claim 28 and the intervening claims are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim contains subject matter, which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Applicant's disclosure fails to recite receiving keys after manufacture. The specification, merely states the key distribution center distributes cryptographic keys to the PGDs and to the distribution centers via a telecommunication network such as the Internet or private link (page 7).

***Claim Rejections - 35 USC § 112***

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter, which the applicant regards as his invention.

Claim 28 and the intervening claims are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

3.1 Regarding claim 28 the phrase "after manufacture" renders the claim(s) indefinite because the claim(s) include(s) elements not actually disclosed. It is not clear what is being manufactured.

***Claim Rejections - 35 USC § 103***

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4.1 **Claims 28-31** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 5,812,666 to **Baker et al.** in view of US Patent 6,058,193 to **Cordery et al.**.

4.2 **As per claim 28, Baker et al** substantially teaches method for dispensing and evidencing indicia by an indicia generating device in a system having a plurality of indicia generating devices that have been divided into n groups, each group corresponding a respective geographic designation each of the indicia generating devices for generating and printing indicia on a media that is to be received at a plurality of establishments, wherein the establishments are associated with different geographic designations, the method performed by the indicia generating devices comprising: (a) receiving postal master key and vendor master key from a key distribution center being communicatively coupled with a vendor and other computers (see column 6, lines 50-56 and figures 3-4) that meets the recitation of receiving a master secret key K and a secret key  $K_i$  after manufacture (see also column 16, line 30 through column 17, line 4 and column 19, lines 1-11) and these keys are stored in the PGD (column 9, lines 33-36); **Baker et al.** also discloses in response to receiving a request to generate an indicium for a medium destined for a particular one of the establishments, generating the indicium (see column 1 and column 3, lines 8-15; column 9, line 55 through column 10, line 21). **Baker et al.** also discloses computing verification keys as a function of the received master keys (see column 5, lines 38-42 and column 17, lines 28 through column 18, line 7), the master keys are also group specific (see column 3, lines 24-32) further discloses that computed verification keys are associated with postal destination to make authentication easier (see column 1, lines 38-50 and column 17, line 64 through column 18, line 35) that meets the recitation of computing a verification key  $V_i$  as a

function of the secret key and the postal destination and computing a key ID as a function of the master secret key and the postal destination. **Baker et al.** also discloses the use of digital signature and the message is sent including the key and the digital signature to determine whether the information contained in the message is correct; in another embodiment a meter produces a digital signature of a key record for integrity and authentication (see column 7, lines 33-58 and column 10, lines 11-21) and also discloses a digital meter signing the key registration record using the vendor and postal master keys so that the vendor and postal domains can trust that the key registration record originated at the digital meter. **Baker et al** even discloses signing the indicia with the digital tokens to provide evidence of payment to the postal and the vendor. To show further evidence that creation of verification key from other keys to generate a digital signature is well known. **Cordery et al.** in an analogous art teaches generating the digital tokens in more details by disclosing that the tokens can be generated by the meter using the received master keys and postal data (column 5, lines 1-17) that includes postal destination (column 2, lines 17-41) so that information can be verified by the correct party (column 5, lines 17-30) and further discloses the meter generating signature using digital token computed from keys received by the meter for verification of indicia and meter specific information (column 2, lines 17-41 and column 3, lines 10-32). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Baker et al.** to use the generated verification key to create a digital signature for the indicia, and digitally signing the indicia by including the digital signature and the other generated token on the indicia because it would allow other party to determine whether both keys can be trusted that they actually originate from the meter. This modification would have been obvious because one skilled in the art would have

Art Unit: 2136

been motivated by the suggestions provided in **Baker et al** and **Cordery et al** to use digital signature so that the key generated for verification of indicia information can be authenticated to ensure that they originate from a trusted meter (see **Cordery et al**, column 2, lines 17-41 and column 3, lines 1-32).

As per claims 29 and 31, **Baker et al.** substantially teaches digital signature using any cryptographic method and combining information about the meter and the mailpiece in the verification process (column 2, lines 1-30). **Cordery et al.** in an analogous art teaches using MAC which is similar to hashing as one of the options of generating digital signature that includes key and postal data as discussed above but other method is suitable as disclosed in **Cordery** (column 7, line 50 through column 8 and column 2, lines 17-41). Computing keys as a one-way function is very well known in the art, for example Schneier in "Applied Cryptography" teaches that with one-way hash function, multiple signatures are easier since the same document can be signed by multiple parties without affecting the size and speed increases signature can be kept separate from the document storage requirement is much smaller. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Baker et al** to use a one-way function to benefit from the advantages known in the art as suggested by Schneier above. Therefore, these claims are rejected on the same rationale as the rejection of claim 28 above.

As per claim 30, **Baker et al.** discloses the limitation of using ZIP codes to designate the postal destination (see column 1, lines 30-50).



*Conclusion*

5. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a). A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the mailing date of this final action.

5.1 The prior art made of record and not relied upon is considered pertinent to applicant's disclosure as the art discloses a multiple device key exchange using asymmetric encryption.

US Patents: 6,636,968 Rosner et al. 6,567,794 Cordery et al ; 5,878,136 Kim et al ; 5,390,251 Pastor et al.

5.2 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2136

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

cc

Carl Colin

Patent Examiner

March 5, 2006

CHRISTOPHER REVAK  
PRIMARY EXAMINER

cel  
3/6/06